Exhibit "A"

Subject: [Fwd: Invention Disclosure Assistance]
Date: Fri, 14 Aug 1998 11:07:30 -0700
From: hja@netscape.com (Harvey Anderson)
To: khikido@netscape.com

98-1140

Subject: Invention Disclosure Assistance
Date: Thu, 13 Aug 1998 17:29:49 -0700 (PDT)
From: prasanta@netscape.com ()
To: hja@netscape.com

This request allows us to assign and track your matter more efficiently; please call Matt Kovac at x2779 for updates on the progress of your request. Below is the result of your feedback form. It was submitted by (prasanta) on Thursday, August 13, 1998 at 17:29:48

Name: Prasanta Behera

Employment status: Employee

Citizenship: india

Home address: 40686 calienete way
fremont, ca 94539

Field of invention: Server Technology

The problem at hand: The Directory server (DS) contains information about people and other useful information like servers. However, the DS is becoming a central repository for user's information Access to those information are controlled by Access Control (ACL) Rules.

Now let's say Netcenter which has 2 million entries for all the Netcenter clients. The Admin of DS will create some basic ACL rules to allow which infromation can be accessed. However there is a need that each user have flexibility to allow the user's information to whoever he wants. For example, I want my hobby information to user x, y & z but nobody else. To achive this, we need to create an ACL rule. SO, if you imagine for @ million user's there will be 2 Million ACL rules. This is not only unmanagable but is very hard to support and perform well.

The solution is to come up with a new scheme where we can achive this functionality using a simple mechanism.

How others solved the problem: At least to my knowledge, I don't know. The obvious choice is to have 1 ACL per entry.

Limitations of #2: The limitations are:
1) hard to manage (too many rules)

Exhibit "A"

2) server penalty on performance.
3) hard for the end users.

My solution: The solution is to support an ACL mechanism where access to the entry is based on the filter value in the proxy attribute. The Admin creates an acl which allowes access based on the proxy attribute's value.

The proxy attribute contains a filter for example, for my entry

dn: uid=prasanta, o=netscape communications corp., c=us
< snip>
allowedbyOwner: (uid=joe)

What this means joe can access to my less private attribute values. In this case, the admin can create an ACL rule like

allow (read) userfilterattr = "allowReadBtOwner".

That's it. Just one RULE. Rcah entry can create a filter (which is an RFC standard) you are done.

How my solution overcomes limitations: You just need to create one ACL rule instead of millions there by for example. Also, it is highly managable and provides better performance.

date of conception: 8/98

Prototype or director's version: Yes ~ Sent

Date of implementation: 8/13

Printed materials about invention: No

Disclosure of invention: No

Plan to sell the invention: No